

Concept de réseau pour la centrale1

Version	Statut	Date	Auteur:in
0.1	Premier projet	20.12.2023	Félix Köppel
0.2	Remaniement	09.01.2024-11.01.2024	Felix Köppel
0.3	Complément selon les mesures	12.01.2024 & 15.01.2024	Felix Köppel
0.4	Compléments	17.01.2024 & 18.01.2024	Felix Köppel
0.5	Petits compléments	24.01.2024 & 25.01.2024	Felix Köppel
0.6	Compléments pare-feu, switch et appareils	02.02.2024	Felix Köppel
0.7	Compléments et attribution de canaux	06.02.2024	Felix Köppel, Fabio Pagotto
0.8	Autres compléments et mise à jour de la planification, mise en place du réseau PVID8	07.03.2024 & 14.03.2024	Felix Köppel
0.81	Mise à jour du statut de l'abonnement Internet	02.05.2024	Felix Köppel
1.0	Dernières finalisations et version finale	PENDING	Egil Rüefli, Felix Köppel, Fabio Pagotto

Ce concept de réseau a été élaboré par l'équipe de projet de Rafisa Informatik GmbH.

Client : Coopérative de construction et d'habitation Kraftwerk1

Hardturmstrasse 134
8005 Zurich

Nom	Fonction	eMail	Téléphone
Andreas Engweiler	Direction	andreas.engweiler@kraftwerk1.ch	044 446 40 66
Alex Hafner	Administration & gestion	alex.hafner@kraftwerk1.ch	044 446 40 64
David Müller	Représentation du maître d'ouvrage (Müller Schnörringer architectes sia)	dm@muellerschnoerringer.ch	044 545 10 66
Andreas Knecht	CEO de l'entreprise d'installation électrique (Züri Elektro AG)	andreas.knecht@zueri-elektro.ch	044 209 92 90

Emplacement de l'objet à équiper

Rue du Hardturm 269
8005 Zurich

Équipe de projet : Rafisa Informatik GmbH

Bernstrasse 88
8953 Dietikon

Nom	Fonction	eMail	Téléphone
Fabio Pagotto	Responsable pare-feu et LAN	f.pagotto@rafisa.ch	+41 76 306 71 51
Felix Köppel	Responsable LAN, pare-feu et WLAN	f.koeppel@rafisa.ch	+41 78 713 43 65
Egil Rüefli	Chef de projet	e.rueefli@rafisa.ch	+41 78 767 84 04

Concept de VLAN et d'adresses IP

Dans ce concept sont indiqués les VLAN-ID, les noms de VLAN et les adresses IP, y compris le masque de sous-réseau, la durée de bail DHCP ainsi que les fonctions des VLAN. Les droits d'accès des VLAN sont également indiqués.

Concept de VLAN & concept de configuration DHCP

Ce concept contient les informations sur les VLAN et les configurations DHCP. Il faut noter ici que le VLAN 10 ne peut pas être utilisé, car ce VLAN est éventuellement nécessaire pour la connexion Internet de Swisscom. Le VLAN 9 est réservé à la connexion Internet fallback. Il faut également noter que ce VLAN n'est conçu que comme un „câble virtuel“ entre la salle des serveurs et le grenier et qu'il est également optionnel.

PVID	Nom du VLAN	Sous-réseau IP	Masque de sous-réseau	Bail	Hôtes (Range)	Fonction
1	VLAN01_MGMT	10.1.1.0	255.255.255.0	30 jours	154 (.100 - .254)	Management VLAN → Gestion de tous les appareils
2	VLAN02_IOT-WR	10.1.2.0	255.255.255.128	30 Jours	30 (.30 - .60)	Réseau uniquement pour onduleur et automate postal
3	VLAN03_IOT-MOB	10.1.3.0	255.255.255.0	1 jour	250 (.3 - .253)	Pour Mobility (Tesla, etc.), station de recharge pour véhicules électriques
4	VLAN04_IOT	10.1.4.0	255.255.255.0	30 jours	250 (.3 - .253)	Tous les appareils IoT
5	VLAN05_GAST	10.1.5.0	255.255.255.0	1 Hour	250 (.3 - .253)	Pour les invités. A des filtres de contenu (contrôle parental et plus)
6	VLAN06_JUGEND	10.1.6.0	255.255.255.0	1 Hour	250 (.3 - .253)	Pour tous les mineurs. A un filtre de contenu (contrôle parental)
7	VLAN07_ERW	10.1.7.0	255.255.255.0	1 Hour	250 (.3 - .253)	Pour les adultes

PVID	Nom du VLAN	Sous-réseau IP	Masque de sous-réseau	Bail	Hôtes (Range)	Fonction
8	VLAN08_FAIRCUS	10.1.8.0	255.255.255.0	1 jour	250 (.3 - .253)	Réseau client équitable
9	VLAN09_FALLBACK	-	-	-	-	Câble virtuel du grenier au pare-feu pour le fallback LTE/5G

Informations de filtrage

Le filtre parental comprend les filtres NSFW et autres auxquels les jeunes ne sont pas autorisés à accéder.

Le filtre supplémentaire dans le réseau d'invités ne met à disposition que la messagerie, les médias sociaux (youtube, instagramm, Facebook et autres), la navigation web, les plateformes vidéo (Netflix et autres).

Matrice d'autorisation des VLAN

VLAN	01	02	03	04	05	06	07	08	09	WAN
01_MGMT	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
02_IOT-WR	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
03_IOT-MOB	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓
04_IOT	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓
05_INVITÉ	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓
06_JEUNESSE	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓
07_ERW	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓
08_FAIRCUS	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓
09_FALLBACK	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗

Plan de réseau SOLL

Les deux plans de réseau ont pour but d'illustrer notre concept. Le plan logique représente la manière dont les appareils communiquent entre eux. Dans le plan de la couche 3, la structure des VLAN proposés est représentée.

Plan de réseau logique

Plan de réseau de la couche 3

Périphériques réseau

Quantité	Appareil	Fabricant	Modèle	Note
1	Modem			Fourni par Init7
1	Pare-feu	Hunsn	RS41	

Quantité	Appareil	Fabricant	Modèle	Note
1	Contrôleur	Ubiquiti Networks	Cloud Key Gen2 Plus	
1	Commutateur	Ubiquiti Networks	USW-24-PoE	
1	Commutateur	Ubiquiti Networks	USW-Flex	Dernier étage
1	Injecteur PoE	Ubiquiti Networks	U-POE-AT	pour switch mansarde
2	Point d'accès	Ubiquiti Networks	U6-Pro	Grenier / Pantouflage, pour ultra haute densité
4	Point d'accès	Ubiquiti Networks	U6-Plus	toutes les autres pièces, pour la basse/moyenne densité
2	Point d'accès	Ubiquiti Networks	UAP-AC-Lite	Garage (WiFi 5 Only pour une meilleure compatibilité avec les terminaux)
1	Point d'accès	Ubnt (ubiquiti networks)	UAP	Périphérique hérité uniquement pour la salle des serveurs - réutilisation d'avant la transformation
1	Injecteur passif PoE	Ubnt (ubiquiti networks)	24 poe passive	Périphérique hérité uniquement pour la salle des serveurs - réutilisation d'avant la transformation

Composants réseau Informations de connexion

Afin d'avoir une meilleure vue d'ensemble de tous les appareils, un tableau a été créé avec les appareils, y compris l'attribution de l'adresse IP et l'accès au VLAN.

Périphérique	Nom d'hôte	PVID	PVID tagué	Adresse IP	Type de connexion	Emplacement	Notes
U6-Pro	ap-kw1-dg	1	3, 4, 5, 6, 7, 8	10.1.1.13	LAN	Grenier	
U6-Pro	ap-kw1-pb	1	3, 4, 5, 6, 7, 8	10.1.1.12	LAN	Bar à pantoufles	
U6-Plus	ap-kw1-kr	1	3, 4, 5, 6, 7, 8	10.1.1.11	LAN	Salle de création	
U6-Plus	ap-kw1-jr	1	3, 4, 5, 6, 7, 8	10.1.1.10	LAN	Salle des jeunes	
U6-Plus	ap-kw1-kd	1	3, 4, 5, 6, 7, 8	10.1.1.9	LAN	Dépôt de consommation	
U6-Plus	ap-kw1-gz	1	3, 4, 5, 6, 7, 8	10.1.1.8	LAN	Chambres d'hôtes	
UAP-AC-Lite	ap-kw1-gn	1	3, 4, 5, 6, 7, 8	10.1.1.7	LAN	Garage (nord)	(WiFi 5 Only)
UAP-AC-Lite	ap-kw1-gs	1	3, 4, 5, 6, 7, 8	10.1.1.6	LAN	Garage (sud)	(WiFi 5 Only)
UAP	ap-kw1-edv	1	7	10.1.1.5	LAN (24passive)	Salle informatique	Appareil LEGACY

Périphérique	Nom d'hôte	PVID	PVID tagué	Adresse IP	Type de connexion	Emplacement	Notes
USW-Flex	sw-kw1-02		1, 2, 3, 4, 5, 6, 7, 8, 9	10.1.1.4	LAN TRUNK	Grenier	
USW-24-PoE	sw-kw1-01		1, 2, 3, 4, 5, 6, 7, 8, 9	10.1.1.3	LAN TRUNK	RK-KW1-01	
Clé Cloud Gen2	uck-kw1-01	1		10.1.1.2	LAN	RK-KW1-01	
Terminaux Fair Customer		8		DHCP	LAN & WiFi	Bureau ()	
Terminaux adultes		7		DHCP	WiFi		
Terminaux Jeunesse		6		DHCP	WiFi		
Terminaux invités		5		DHCP	WiFi		
Terminaux IoT		4		DHCP	WiFi		
TV au dernier étage		4		DHCP	LAN	Grenier	
Appareils de mobilité		3		DHCP	WiFi	Garage	

Liste des terminaux : Connectivité

Liste des terminaux

Le tableau suivant contient tous les types d'appareils utilisés avec les possibilités de connexion possibles et celles que nous recommandons (ou que nous avons déterminées lors de réunions).

Nombre	Marque	Nom de l'appareil	Type d'appareil	Fonctionnalité IT	Proposition Connexion	Emplacement
			Onduleur	Ethernet/WiFi	Ethernet	
			E-mobile	WiFi	WiFi	Garage

Liste des terminaux : Connexion réseau

Nom/marque de l'appareil	Type d'appareil	Type de connexion	PVID	Attribution d'adresse IP	Nom d'hôte
	Onduleur	LAN	2	DHCP	-
	E-mobile	LTE/WiFi	3	DHCP	-

Switch Allocation de port VLAN

Modifications possibles, pas encore définitives !

sw-kw1-01

Modèle de switch : USW-24-POE Ubiquiti Networks Switch 24 PoE Standard

Budget PoE : 95 watts. Total utilisé : 75 watts.

Port	Patch	PVID (natif/[tagué]/{profil})	Périphérique	Adresse MAC	Puissance	Nom d'hôte / note
1	-	1	Ordinateur portable de gestion			Gestion uniquement
2	-					LIBRE
3	UG04					
4	CE07					
5	EG05					
6	EG06					
7	EG04					
8	UG02					
9	-	1 - UCK	Clé Cloud Gen2 Plus	70:a7:41:f9:65:63	13 Watt	uck-kw1-01 (RK-KW1-01)
10	UG03	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	UAP-AC-Lite	d8:b3:70:b6:a7:b8	6.5 Watt	ap-kw1-gs / Garage Sud (WiFi 5 Only)
11	UG01	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	UAP-AC-Lite	d8:b3:70:b6:a8:16	6.5 Watt	ap-kw1-gn / Garage Nord (WiFi 5 Only)
12	EG01	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	U6-Plus	d8:b3:70:e9:34:3c	9 watts	ap-kw1-gz / chambre d'amis
13	CE12	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	U6-Plus	d8:b3:70:e6:d9:40	9 watts	ap-kw1-kd / Dépôt de consommation
14	EG11	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	U6-Plus	d8:b3:70:e9:06:68	9 watts	ap-kw1-jr / Salle des jeunes
15	CE02	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	U6-Plus	d8:b3:70:e9:4d:60	9 watts	ap-kw1-kr / Salle de création
16	EG03	1 [3, 4, 5, 6, 7, 8] {AP-Uplink}	U6-Pro	e4:38:83:6b:47:31	13 watts	ap-kw1-pb / Bar à pantoufles
17	-	1 [7, 8] - AP-EDV	UAP	24:a4:3c:86:6c:e4	-	ap-kw1-edv / EDV-AP. Injecteur PoE passif 24v
18	EG09				-	FAIR CUSTOMER
19	EG08				-	POSTE DE PAQUET
20	EG10				-	FAIR CUSTOMER

Port	Patch	PVID (natif/[tagué]/{profil})	Périphérique	Adresse MAC	Puissance	Nom d'hôte / note
21	DG01				-	RÉSERVE GRENIER
22	DG02	TRUNK {UPLINK}	USW-Flex Port 1	ac:8b:a9:a5:ed:0e	-	Injecteur PoE+ alimenté, liaison montante SW- KW1-02
23	-	TRUNK {UPLINK}	Pare-feu LAN2		-	Réservé - Link aggregation Firewall ! - Désactivé
24	-	TRUNK {UPLINK}	Pare-feu LAN1		-	Main Uplink vers le pare-feu

sw-kw1-02

Port	PVID (non balisé/[balisé]/{profil})	Périphérique	Adresse MAC	Consommation d'énergie	Nom de l'appareil/notice
1	TRUNK	Switch salle de serveurs	d8:b3:70:5c:fd:77	Entrée d'alimentation	Injecteur PoE+
2	7	indéterminé		-	inconnu
3	7	Armoire Raccordement au réseau		-	Raccordement dans l'armoire
4	7	Raccordement au réseau électrique Table		-	Raccordement table
5	1 [3, 4, 5, 6, 7, 8] {AP- Uplink}	U6-Pro	e4:38:83:72:96:71	13 watts	ap-kw1-dg

On pourrait définir le profil TRUNK sur le port 4 et brancher un USW-Flex Mini, qui ne consomme que 2,5 watts, et le configurer en fonction des besoins pour avoir plus de ports Ethernet.

SSID WiFi, bandes de fréquences et attribution VLAN

Felix a noté ici les SSID WiFi (noms de réseau WiFi), le type de cryptage, l'allocation VLAN et les bandes de fréquence radio. Felix a également noté la limitation de la bande passante pour le réseau. Ici, les indications sont données du point de vue du client, c'est-à-dire que 20/30 (up/dn) correspondrait à 20Mbit/s en upload et 30Mbit/s en download.

Shared Key est une nouvelle technologie qui permet d'avoir un SSID et plusieurs mots de passe. Selon le mot de passe saisi, on accède à l'un ou l'autre VLAN. Il est possible d'enregistrer plusieurs mots de passe et de déterminer dans quel VLAN ils seront utilisés.

SSID	PVID	Bande de fréquence	Cryptage	Groupe AP	Appareils	QoS (Mbit/s)	Autre
KW1-DEBUG	1	2.4GHz & 5GHz	WPA3-SAE	All	Admins & appareils de test	illimité	actif uniquement lors du débogage
KW1-Mobilité	3	2.4GHz & 5GHz	WPA2-PSK	GARAGE	Voitures, terminaux Mobility	40/40 (up/dn)	Actif
KW1	1, 4, 5, 6, 7, 8	2.4GHz & 5GHz	WPA2-PSK	All	Tous les appareils	50/50 (up/dn)	Actif avec clé partagée
KW1-EDV	7	2.4GHz	WPA2-PSK	INFORMATIQUE	Admins dans la salle informatique	illimité	Uniquement sur AP dans la salle informatique Active !

Paramètres radio

		Bande de fréquence 2.4GHz			Bande de fréquence 5GHz			
Nom d'hôte AP	Groupe AP	Canal	Bande passante	Puissance TX	Canal	Bande passante	TX-Power	Autre
ap-kw1-edv	EDV	Auto	20MHz	23dBm	-	-	-	2.4GHz seulement
ap-kw1-gn	GARAGE, GN	9	20MHz	20dBm	48	80MHz	20dBm	WiFi 5 seulement
ap-kw1-gs	GARAGE, GS	5	20MHz	20dBm	64	80MHz	20dBm	WiFi 5 seulement
ap-kw1-kd	KD, tout	13	20MHz	17dBm	64	40MHz	23dBm	
ap-kw1-gz	GZ, All	1	20 MHz	17dBm	136	40MHz	23dBm	
ap-kw1-jr	JR, All	5	20MHz	26dbm	136	40MHz	26dBm	Décharge KR
ap-kw1-kr	KR, All	1	20MHz	26dBm	52	80MHz	26dBm	Décharge PB
ap-kw1-pb	PB, All	5	20MHz	22dBm	128	80MHz	26dBm	Mode extérieur
ap-kw1-dg	DG, All	5	20MHz	22dBm	128	80MHz	26dBm	Mode extérieur

Configurations VPN

En cours d'ajout !

Connexion Internet

En phase de réalisation.

Mise à niveau vers init7 Fiber 1/1 gbit/s avec media Converter et abonnement TV - confirmé !
Commande en cours.

actuellement : raccordement Swisscom Fibre 40/40 mbit/s avec Swisscom Internet Box Standard

Solution de repli

Opérateur de téléphonie mobile/abonnement : Inconnu Modem 4G/5G : En cours d'ajout !

A compléter !

IPTV

A compléter !

Existant Blue TV avec abonnement sportif

Documentation des réglages

https://wiki.rafisa.net/doku.php?id=de:intern:dokumentationen:log_unifi-cloud-key_access-point_konfigurieren

From:

<https://wiki.rafisa.net/> -

Permanent link:

https://wiki.rafisa.net/doku.php?id=fr:intern:kw1_network-concept

Last update: **2024/05/02 11:21**

